CORE
Metadata, citation and similar papers at core.ac.uk
Provided by University of Southern Queensland ePrints

Security modelling for e-Learning

Jianming Yong
School of Information Systems
Faculty of Business, University of Southern Queensland, AUSTRALIA
yongj@usq.edu.au

Abstract

As more and more organisations and institutions are moving towards the e-learning strategy, the security issue becomes a big challenge. This paper addresses this challenge and works out a new mechanism to implement security modelling for e-learning. Under this new security modelling, e-learning systems can be better implemented by all stakeholders.

Keywords: Security mechanism, E-learning, ERBAC,

1. Introduction

E-learning is becoming one of most important educational means. As more and more educational organisations are moving into e-learning, some organisations are pushing a uniform standard to facilitate e-learning implementation. Currently there are four main e-learning standard organisations: AICC [1], IEEE Learning Technology standards Committee [2], IMS Globe Consortium [3] and ADL [4].

AICC is an international group of technology-based training professionals that creates CBT-related guidelines for the aviation industry. AICC publishes a variety of recommendations, but its standards with the most impact on the e-learning arena are its computer-managed instruction (CMI) guidelines.

IEEE is an international organization that develops technical standards and recommendations for electrical, electronic, computer and communication systems. Within the IEEE, the Learning Technology Standards Committee (LTSC) provides specifications that address best practices, which can be tested for conformance. Basically, they wrote the standard on how to write standards. The most widely acknowledged IEEE LTSC specification is the Learning Object Metadata (LOM) specification, which defines element groups and elements that describe learning resources.

IMS Global Consortium is a consortium of suppliers that focus on the development of specifications that focus on the use of metadata to address content packaging. The specifications are used to define how an LMS communicates with back-end applications and content objects or libraries. Several of its standards are made available on its website at no fee.

ADL is a U.S. government-sponsored organization that researches and develops specifications to encourage the adoption and advancement of e-learning. The most widely accepted ADL publication is the ADL Shareable Content Object Reference Model (SCORM). SCORM defines a Web-based learning 'Content Aggregation Model' and 'Run-Time Environment' for learning objects. SCORM is a collection of specifications adapted from best practices of various existing e-learning standards to provide a comprehensive suite of e-learning capabilities that enable interoperability, accessibility and reusability of Web-based learning content. The SCORM specification combines the best elements of IEEE, AICC, and IMS specifications into a consolidated document.

Many countries are trying to define their own e-learning standards/frameworks. Like Australia [5], a flexible learning framework is designed to support e-learning strategy. European Union has Alliance of Remote Instructional Authoring and Distribution networks for Europe (ARIADE) [6] to support e-learning strategy.

Almost all e-learning standards/frameworks are focusing on e-learning system design, course development and delivery, system interoperability and scalability. The security concerns have not caused enough attention by these e-learning initiatives as many e-learning projects are still under the trials. While more and more e-learning systems are formally used by educational institutions and more and more e-learning systems adopt open source technology, the e-learning security concerns become inevitable. The paper tries to systematically address right access control mechanism for e-learning.

This paper is organised as the follows. Section 2 will discuss our recent contribution towards RBAC. Section

3 will analyse specific roles and attributes which is much relevant to e-learning. Section 4 will address Architecture of security modelling for e-learning system. Section 5 will conclude the paper.

2. Extended RBAC (ERBAC)

The most fundamental concept of RBAC is the role. The role decides the security properties of information systems. It is important to do further research on the role. So far there are some further researches on the role, like environment role [7], parameterized role [8], and attributed role [9].

In [7], the environment role is defined as a role which is use to capture environmental conditions. The environment role has extended the traditional RBAC with a new type of role. When the users get their roles, they have to get support from relevant environment roles so that they can successfully execute their assigned roles. In [8], a role is associated with a template. A role template is represented as follows:

$$r(\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \ldots \chi_n)$$

Where r is the role name and $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \ldots \chi_n$ are properties bound to the role, also called parameters of the role. In [9], the role attributes are defined, the notion of role attributes is very similar to the role parameters [5]. Unfortunately none of further research has been done to extend role attributes into RBAC. We are realising that the role attributes can be used to rebuild RBAC and to further enhance the central concept of the role. In the following sections, we will address the role attribute in details. The role attributes will have a big impact to current RBAC mechanism. Also the individual role's privacy can also be protected by an effective implementation of role attributes.

A role consists of various attributes which demonstrate the property of the role and the permissions the role holds. In order to clearly descript how the role attributes to have the impacts on current RBAC mechanism, we need a further discussion on the role attributes as follows. In order to clearly demonstrate our intention, this paper directly refers to some definitions from [10] as the follows.

Definition of Attribute
Definition 1 (Attribute) An attribute (Attr) is a property of a role (r). A set of relevant attributes consists of a role. A role has a fix set of attributes. The relationships between the role and the attribute are presented as follows:

$$r(Attr) = r(Attr_0, Attr_1, \ldots, Attr_n)$$

$$\forall\ Attr_i, Attr_j \in r,\ 0 \le i \le n,\ 0 \le j \le n : \text{if } i \ne j,$$

$$\text{then } Attr_i \cap Attr_j = \Phi$$

$$\bigcup_{i=0}^{n} Attr_i = r(Attr)$$

If a system has a set of roles, R, $R=R(r_0, r_1, r_2, \ldots, r_m)$, and ATTR is as a full set of attributes for the system, we will have the following relationship:

$$ATTR = r_0(Attr) \cup r_1(Attr) \cup \ldots \cup r_m(Attr)$$

In order to use the role attributes to implement access control, we need to define more concepts to support this mechanism.

Attributes types
As the attributes are properties of a role, we define four types of attributes: compulsory, optional, obvious, and hidden.

Compulsory
Definition 2 (Compulsory Attribute (CA)) A compulsory attribute is an essential part of a role. If a compulsory attribute of a role is deactivated or a compulsory attribute has an empty value, the role cannot be assigned to any user and the role is also in a non-active situation.

$$\forall\ Attr_k \in ATTR,\ 0 \le k \le z,\ z \text{ is the cardinality of ATTR}$$

$$\text{If } Attr_k \in r(Attr) \text{ and } Attr_k \text{ is a CA of } r$$

$$\text{Then } Attr_k \leftrightarrow r(Attr)$$

Optional
Definition 3 (Optional Attribute (OA)) An optional attribute is not an essential part of a role. If an OA of a role is deactivated or an OA has an empty value, the role can still be assigned to the users for a normal execution.

$$\forall\ Attr_k \in ATTR,\ 0 \le k \le z,\ z \text{ is the cardinality of ATTR}$$

$$\text{If } Attr_k \in r(Attr) \text{ and } Attr_k \text{ is an OA of } r$$

$$\text{Then } Attr_k \mapsto r(Attr)$$

Obvious
Definition 4 (Obvious Attribute (ObA)) An obvious attribute of a role is visible to all other roles which have relationships with this role. ObA can be useful in the hierarchical RBAC and constraint RBAC. ObA can be formulized as the follows:

$$\forall\ Attr_k \in ATTR,\ 0 \le k \le z,\ z \text{ is the cardinality of ATTR}$$

$$\text{If } Attr_k \in r_i(Attr) \text{ and } Attr_k \text{ is an ObA of } r_i \text{ and}$$

If r_i x r_j $\neq \Phi$ & $i \neq j$ Then $Attr_k$ is visible to r_j

Hidden

Definition 5 (Hidden Attribute (HA)) A hidden attribute of a role is only visible to the role itself. It can be expressed as follows:

$\forall$ $Attr_k \in ATTR$, $0 \leq k \leq z$, z is the cardinality of ATTR

If $Attr_k \in r_i(Attr)$ and $Attr_k$ is an ObA of r_i and

If r_i x r_j $\neq \Phi$ & $i = j$ Then $Attr_k$ is visible to r_j

Other $Attr_k$ is never visible to r_j

Role conformation

Based on four role types, a role can be formed by only CA or CA as well as OA. Any CA can be ObA or HA. Any OA can also be ObA or HA. The role formation is shown at Figure 1.

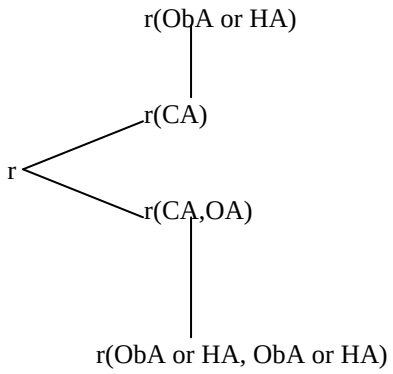

Figure 1 Role conformation

3. Security roles and attributes related to e-learning

When e-learning systems are needed for educational institutions, there are different stakeholders/interested parties involved, like developers, institutions, regulators, instructors, administration staff, supporting technicians, learners. It is important to classify the security roles and relevant attributes of all stakeholders respectively.

Developers

Developers are in charge of designing, building and testing e-learning system. The attributes of developers' role have to be included as the following table.

Type selection / Attributes name and description	CA	OA	ObA	HA
System Security architecture design (D1)	R	N/A	A	U
Access Control mechanism (D2)	R	N/A	A	U
Privacy policy implementation (D3)	R	N/A	A	U
Data integrity assurance (D4)	R	N/A	A	U
Confidentiality assurance (D5)	R	N/A	A	U
Availability assurance (D6)	R	N/A	A	U
Identification mechanism (D7)	R	N/A	A	U
Authentication assurance (D8)	R	N/A	A	U
Accountability assurance (D9)	R	N/A	A	U
Non-repudiation mechanism (D10)	R	N/A	A	U
Cryptography implementation (D11)	A	A	A	U
Copyright protection (D12)	A	A	A	A
R-Required, N/A- Not applicable, A-Acceptable, U-Unacceptable				

Institutions

Institutions normally give a general requirement of e-learning system. They might not be able to identify any specific security needs and their attributes for security are listed in the following table.

Type selection / Attributes name and description	CA	OA	ObA	HA
System general security requirements (I1)	R	N/A	A	A
Security policy (I2)	R	N/A	A	A
Privacy policy (I3)	R	N/A	A	A
Incident plan (I4)	R	N/A	A	A
Disaster plan (I5)	R	N/A	A	A

System continuity plan (I6)	R	N/A	A	A
Identification policy (I7)	R	N/A	A	A
Authentication policy (I8)	R	N/A	A	A
Accountability hierarchy (I9)	R	N/A	A	A
R-Required, N/A- Not applicable, A-Acceptable, U-Unacceptable				

Regulators

Regulators are in charge overall security and privacy policy through legislation. The security attributes of regulators are mainly included in the following table.

Type selection / Attributes name and description	CA	OA	ObA	HA
Security forensic legislation (R1)	R	N/A	A	U
Privacy legislation (R2)	R	N/A	A	U
R-Required, N/A- Not applicable, A-Acceptable, U-Unacceptable				

E-learning system users

Instructors are in charge of course production and delivery via e-learning system. Administration staff are in charge of administration functions of e-learning system, like student enrolments, etc. Supporting technicians are in charge of maintaining e-learning systems as the technical support. Learners are those who use e-learning systems to conduct their learning. As they are all e-learning system users, their security attributes depend on developers, institutions, and regulators.

Type selection / Attributes name and description	Instructor	Learner	Admin staff	Technician
System Security architecture design (D1)	A	A	A	R
Access Control mechanism (D2)	A	A	A	R
Privacy policy implementation (D3)	A	A	A	R
Data integrity assurance (D4)	A	A	A	R
Confidentiality assurance (D5)	A	A	A	R
Availability assurance (D6)	A	A	A	R
Identification mechanism (D7)	A	A	A	R
Authentication assurance (D8)	A	A	A	R
Accountability assurance (D9)	A	A	A	R
Non-repudiation mechanism (D10)	A	A	A	R
Cryptography implementation (D11)	A	A	A	R
Copyright protection (D12)	A	A	A	R
System general security requirements (I1)	A	N/A	A	R
Security policy (I2)	A	N/A	A	R
Privacy policy (I3)	A	N/A	A	R
Incident plan (I4)	A	N/A	A	R
Disaster plan (I5)	A	N/A	A	R
System continuity plan (I6)	A	N/A	A	R
Identification policy (I7)	A	N/A	A	R
Authentication policy (I8)	A	N/A	A	R
Accountability hierarchy (I9)	A	N/A	A	R
Security forensic legislation (R1)	A	U	A	R

Privacy legislation (R2)	A	U	A	R
R-Required, N/A- Not applicable, A-Acceptable, U-Unacceptable				

From the immediately previous table, the supporting technicians are taking a main security responsibility and the instructors and administration staff also significantly impact on the e-learning security. The students only impact on the e-learning system security via developers' assignments.

4. Architecture of security modelling for e-learning system

From the previous section, we have a clear picture of all stakeholders of e-learning systems and their security attributes directly impact on the security design, implementation and maintenance. Picture 2 shows the relationships and dependency of security architecture for e-learning systems.

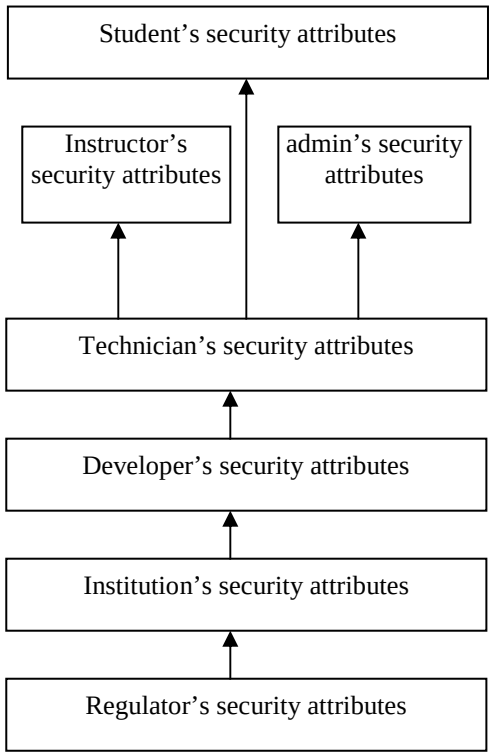

Figure 2 Security modelling of e-learning

Figure 2 illustrates the regulator's security attributes will decide and influence the security attributes of e-learning institutions. The institution's security attributes will decide and influence the security attributes of e-learning developers. The developer's security attributes will decide and influence the security attributes of e-learning technicians. The technician' security attributes will decide and influence the security attributes of e-leaning instructors, administration staff and learner. The instructor's security attributes and administration staff's security attributes will decide and influence the security attributes of e-learning learners.

5. Conclusion remarks

This paper discusses the security attributes which are relevant to all e-learning stakeholders, regulator, institution, developer, instructor, administration staff, instructor and learners. A security modelling for e-learning system illustrates the relationships among e-learning stakeholders. This is still earlier stage to apply separated security attributes to overall e-learning system. More research needs to be done on how these security attributes can be effectively applied and connected with current e-learning standards, like AICC, IEEE LTSC, IMS, ADL, etc. We expect more research on the e-learning security and privacy.

References

1 AICC, Aviation Industry CBT (Computer-Based Training) Committee (AICC), online, http://www.aicc.org

2 IEEE LTSC, The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board, online, http://ieeeltsc.org/

3 IMS, Instructional Management Systems Global Consortium, online, http://www.imsglobal.org/

4 ADL, Advanced Distributed Learning , online, http://www.adlnet.gov/

5 Australian Flexible learning framework, online, http://e-standards.flexiblelearning.net.au/docs/vet-eportfolio-report-v1-0.pdd

6 ARIADNE, A European Association open to the World, for Knowledge Sharing and Reuse, online, http://www.ariadne-eu.org/

7 Michael J. Covington, Wende Long, Srividhya Srinivasan, Anind K. Dey, Mustaque Ahamed, and Gregory D. Abowd, Securing Context-Aware Applications Using Environment Roles, In Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, pages 10-20, May 2003, Chantilly, Virginia, USA.

8 Luigi Giuri and Pietro Iglio, Rold Templates for Content-Based Access Control, *In Proceedings of the second ACM Workshop on Role-Based Access Control*, pages 153-159, 1997, Fairfax, Virginia, USA.

9 Ji-Won Byun, Elisa Bertino, and Ninghui Li, Purpose Based Access Control of Complex

Data for Privacy Proctection, *In Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, pages 102-110, June 2005, Stockholm, Sweden.

10 Jianming Yong, Elisa Bertino, Mark Toleman, Dave Roberts, Extended RBAC with Role Attributes, The 10th Pacific Asia Conference on Information Systems, Accepted as a full paper, pp457-469, July 6-9, Kuala Lumpur , Malaysia